UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,747	10/31/2001	Richard Paul Tarquini	10014006-1	4897

7590   04/28/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
PERUNGAVOOR, VENKATANARAY

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2001*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
    closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8 and 15* is/are allowed.

6)☐ Claim(s) *1-7,9-14 and 16-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Specifications

1. The "Cross Reference To Related Applications" contains blanks to the

   Application Number. The Examiner suggests the Applicant fill in the related

   Applications appropriately. Appropriate correction required.

Claim Rejections –35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

   form the basis for the rejections under this section made in this Office action:

   A person shall be entitled to a patent unless –

3. (e) the invention was described in (1) an application for patent, published under section 122(b), by
   another filed in the United States before the invention by the applicant for patent or (2) a patent
   granted on an application for patent by another filed in the United States before the invention by the
   applicant for patent, except that an international application filed under the treaty defined in section
   351(a) shall have the effects for purposes of this subsection of an application filed in the United States
   only if the international application designated the United States and was published under Article 21(2)
   of such treaty in the English language.

   5- 4, 15, 16 are

4. Claim 1, 5-7, 9, 16 rejected under 35 U.S.C. 102(e) as being anticipated by U.S.

   Patent 6279113 to Vaidya.

5. Regarding Claim 1, Vaidya discloses the an intrusion detection system whereby

   the all the seven OSI layers are monitored; which includes the application,

   transport and network layer see Col 4 Line 29-31.

6. Regarding Claim 5, Vaidya discloses the first layer(application layer) interfacing

   with the file system. Vaidya discloses having an memory of profiles and this

   profile interfacing with application session see Col 4 Line 8-10 & Line 19-22.

7. Regarding Claim 6, Vaidya discloses the file system interfacing with the first layer which includes an database for storing reports and signature file see Col 3 Line 66- Col 4 Line 39.

8. Regarding Claim 7, Vaidya discloses the first layer(application layer) providing the third layer(network layer) the signature files see Col 3 Line 40-48.

9. Regarding Claim 8, Vaidya discloses the communication session between intrusion prevention system and database system see Col 2 Line 30-53.

10. Regarding Claim 9, Vaidya discloses the an intrusion detection system whereby the all the seven OSI layers are monitored; which includes the application, transport and network layer see Col 4 Line 29-31. Vaidya also discloses the instructions and processor see Col 6 Line 11-25.

11. Claim 15 is rejected under the same rationale as Claim 8 above.

12. Regarding Claim 16, Vaidya discloses the archiving of intrusion related events in a database file system see Col 4 Line 8-18 & Col 5 Line 47-51.

Claim Rejections – 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claim 2,3,4,10-13, 17-19 rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent 6279113 to Vaidya in view of U.S. 6851061 B1 to Holland III et

al.

15. Regarding 2, 3 and 4, Vaidya does not disclose the use of drivers to monitor

network layer, transport layer interface and first layer interfacing with the second

layer by a dynamically linked library. However, Holland et al. discloses the use of

filter to monitor the network layer see Column 4 Line 52-67; further discloses the

use of an audit system to monitor transport layer see Column 4 Line 31-52; and

also discloses the use of dynamically linked library for interfacing with the first

and second layer see Col 5 Line 61-Col 6 Line 15.It would be obvious to one

having ordinary skill in the art at the time of the invention to include use of drivers

to monitor network layer, transport layer interface and first layer interfacing with

the second layer by a dynamically linked library in the invention of Vaidya in

order to increase internal security and latency as taught in Holland see Col 4 Line

2-19.

16. Regarding Claim 10,12, and 13, are rejected under the same rationale as Claim
2, 3 and 4 above.

17. Regarding Claim 11, Vaidya does not disclose the initialization of stack.
However, Holland et al. discloses the initialization see Col 4 Line 43-67. It would
be obvious to one having ordinary skill in the art at the time of the invention to
include initialization of stack in the invention of Vaidya in order to have an clean
stack for data to be put upon.

18. Regarding Claim 17, Vaidya discloses an processor, memory module see
Column 6 Line 1-26 & Col 5 Line 47-67, but does not disclose the use of drivers
to monitor network layer, transport layer interface and first layer interfacing with
the second layer by a dynamically linked library. However, Holland et al.
discloses the use of filter to monitor the network layer see Column 4 Line 52-67;
further discloses the use of an audit system to monitor transport layer see
Column 4 Line 31-52; and also discloses the use of dynamically linked library for
interfacing with the first and second layer see Col 5 Line 61-Col 6 Line 15.It
would be obvious to one having ordinary skill in the art at the time of the
invention to include use of drivers to monitor network layer, transport layer
interface and first layer interfacing with the second layer by a dynamically linked
library in the invention of Vaidya in order to increase internal security and latency
as taught in Holland see Col 4 Line 2-19.

19. Regarding Claim 18, Vaidya discloses the intrusion protection system
communicating with the file system see Col 5 Line 27-33.

20. Regarding Claim 19, Vaidya discloses the logging of intrusion-related data in
database for future reference see Col 5 Line 47-50.

Conclusion

21. Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Venkatanarayanan Perungavoor whose
telephone number is 571-272-7213. The examiner can normally be reached on
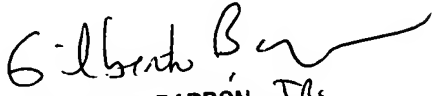8-4:30.

21. If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone
number for the organization where this application or proceeding is assigned is 703-
872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

VP
4/08/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100